Shared Service System Audits: What User Management and Auditors Need to Know

JFMIP
May 2014

Presented by:

Robert Dacey – GAO

Session Objectives

- Properly using SSAE 16 service organization audit reports
- Revisions to SSAE 16 that are currently under consideration by the AICPA

Background

- Using shared services affects the user entity’s controls over financial reporting
- While the service organization implements common controls over financial reporting and can provide information on the effectiveness of those controls, user entities remain responsible for determining whether their internal control over financial reporting is effective, including consideration of all service and subservice organizations

User Auditor Responsibilities

- Obtain an understanding of the nature and significance of the services provided by the service organization and their effect on the user entity's internal control relevant to the audit, sufficient to identify and assess the risks of material misstatement.
- Design and perform audit procedures responsive to those risks.

User Entity Management Responsibilities

- As part of A-123, user entity management is ultimately responsible for the internal control over financial reporting, including information processed by service organizations.

Are the Service Organization's Services Part of the User Entity's Information System?

Yes, if these services affect any of the following:

a. The classes of transactions in the user entity's operations that are significant to the user entity's financial statements;

b. The procedures within both IT and manual systems by which the user entity's transactions are initiated, authorized, recorded, processed, corrected as necessary, transferred to the general ledger, and reported in the financial statements;

c. The related accounting records, supporting information, and specific accounts in the user entity's financial statements that are used to initiate, authorize, record, process, and report the user entity's transactions;

Are the Service Organization's Services Part of the User Entity's Information System (cont’d)

Yes, if these services affect any of the following (cont’d):

d. How the user entity's information system captures events and conditions, other than transactions, that are significant to the financial statements;

e. The financial reporting process used to prepare the user entity's financial statements, including significant accounting estimates and disclosures; and

f. Controls surrounding journal entries, including nonstandard journal entries used to record nonrecurring, unusual transactions, or adjustments.

Excluded Services

Does not apply to services that are limited to processing an entity's transactions that are specifically authorized by the entity, such as

- processing of checking account transactions by a bank, or
- the processing of securities transactions by a broker (when the user entity retains responsibility for authorizing the transactions and maintaining the related accountability).

If a service organization's services part of the user entity's information system, what should the user entity and user auditor know about the services provided by the service organization?

An Understanding of the Services Provided by the Service Organization

- The nature of the services provided by the service organization and the significance of those services to the user entity, including their effect on the user entity's internal control
- The nature and materiality of the transactions processed or accounts or financial reporting processes affected by the service organization
- The degree of interaction between the activities of the service organization and those of the user entity
- The nature of the relationship between the user entity and the service organization, including the relevant contractual terms for the activities undertaken by the service organization

Can the User Entity Have Controls Over the Transactions Processed by the Service Organization?

- Yes, both monitoring controls and controls over the reliability of the data processed by the service organization

- The user auditor should evaluate the design and implementation of relevant controls at the user entity that relate to the services provided by the service organization, including those that are applied to the transactions processed by the service organization.

How Can the User Entity and User Auditor Obtain Sufficient Information About the Services Provided?

- Obtaining and reading a type 1 or type 2 report, if available
- Contacting the service organization, through the user entity, to obtain specific information
- Visiting the service organization and performing procedures that will provide the necessary information about the relevant controls at the service organization
- Using another auditor to perform procedures that will provide the necessary information about the relevant controls at the service organization

Is There More Than One Type of Service Organization Control (SOC) Report?

Yes, be sure to use the right one

- **SOC 1** **-** Report on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting
  - AICPA audit guide

- **SOC 2** Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality and/or Privacy
  - AICPA audit guide

- **SOC 3** Trust Services Report
  - Webtrust, Systrust

What Should I know About the Service Auditor and Audit?

- The service auditor's professional competence and independence from the service organization
- The adequacy of the standards under which the report was issued (e.g., AICPA, IAASB)

Does the SOC 1 Report Cover An Appropriate Period?

- Compare the period covered by the type 2 report to the user entity's financial reporting period
- If little overlap exists between the period covered by the type 2 report and the period for which the user auditor intends to rely on the report,
  - an additional type 2 report covering a preceding or subsequent period may provide additional audit evidence, or
  - it may be necessary to perform, or use another auditor to perform, tests of controls at the service organization in order to obtain sufficient appropriate audit evidence about the operating effectiveness of those controls.

What Additional Evidence Do I Need If There Are Periods Not Covered by a Service Auditor Report?

Relevant factors in determining what additional evidence to obtain about control effectiveness for periods not covered by a service auditor's report may include the following:

- The significance of the assessed risks of material misstatement at the assertion level
- The specific controls that were tested during the interim period and significant changes to them since they were tested including changes in the information systems, processes, and personnel
- The degree to which audit evidence about the operating effectiveness of those controls was obtained
- The length of the remaining period
- The effectiveness of the control environment and monitoring controls at the user entity
- The extent to which the user auditor intends to reduce further substantive procedures based on the reliance on controls

When Looking at a SOC 1 Report, What Should I Read First?

- Read the opinions
  - Fair presentation of the description of the service organization’s system
  - Suitability of the design of the service organization controls
  - For type 2 engagements, operating effectiveness of the service organization controls
- What are the opinions (unmodified, qualified, adverse,disclaimer) ?
- Understand any explanatory paragraphs (e.g., reasons for report modifications)?

Once I See That the opinions Are Unmodified, Am I Done?

- No, further procedures are necessary

What If The Opinions Are Not Unmodified?

- Deviations noted by the service auditor or matters giving rise to a modified opinion in the service auditor's report are considered in the assessment of the tests of controls performed by the service auditor.
- Consider discussing such matters with the service auditor.

Are There Subservice Organizations?

- If so, which method is used?
  - Inclusive method – method of addressing services provided by a subservice organization (SSO) whereby management's description includes the nature of services provided by the SSO as well as relevant control objectives and controls, or
  - Carve out method – method of addressing services provided by a SSO whereby management's description of the system excludes the SSO's control objectives and controls.
- For each subservice organization that is carved out, perform all of the procedures that are applied to the service organization

Are There Complementary User Entity Controls?

- **Complementary user entity controls.** Controls that management of the service organization assumes, in the design of its service, will be implemented by user entities, and which, if necessary to achieve the control objectives stated in management's description of the service organization's system, are identified as such in that description.

What Do I Do if There Are Complementary user Entity Controls?

- Determine whether complementary user entity controls are relevant in addressing the risks of material misstatement relating to the relevant assertions in the user entity's financial statements
- If so, determine whether the user entity has designed and implemented such controls and, if so, testing their operating effectiveness

Are The Control Objectives Appropriate?

- Service auditor vs. user entity/user auditor responsibilities

What Is The Service Auditor Responsible For?

- Are the control objectives stated in the description reasonable in the circumstances
  - Do the control objectives relate to the types of assertions commonly embodied in the broad range of user entities' financial statements to which controls at the service organization could reasonably be expected to relate (for example, assertions about existence and accuracy that are affected by access controls that prevent or detect unauthorized access to the system)?
  - Are the control objectives complete?
- Control objectives that are reasonable in the circumstances should relate to controls that are likely to be relevant to user entities' internal control over financial reporting.

What Is Entity Management Responsible For?

- It is the responsibility of individual user entities or user auditors to assess whether the control objectives included in the description are relevant and sufficient to meet their needs.
- Consider control objectives the user entity would use if the service organization processing was performed by the user entity

What Should I do With Respect to the Control Testing?

- Read the control tests and test results
- Consider whether the tests are sufficient to meet the user’s needs
- Consider the impact of any testing deviations

Other Considerations When Using a Service Auditor’s Report

- Has the service organization reported or is user entity management otherwise aware any fraud, noncompliance with laws and regulations, or uncorrected misstatements affecting the financial statements of the user entity ?
- Use of IT specialists
- Overall sufficiency and appropriateness of the evidence provided by the report

Service Auditor’s Consideration of Intentional Acts

- The risks and control objectives encompass intentional and unintentional acts that threaten the achievement of the control objectives
- If the service auditor becomes aware that the deviations resulted from intentional acts by service organization personnel, the service auditor should assess the risk that the description of the service organization’s system is not fairly presented and that the controls are not suitably designed or operating effectively.
- Require written representations from management that it has disclosed to the service auditor knowledge of any actual, suspected, or alleged intentional acts by management or the service organization’s employees, of which it is aware, that could adversely affect the description or the completeness or achievement of the control objectives stated in the description.

Service Auditor’s Consideration of Noncompliance, Fraud, or Uncorrected Errors

- If the service auditor becomes aware of noncompliance, fraud, or uncorrected errors:
  - Determine the effect of such incidents on the description of the service organization’s system, the achievement of the control objectives, and the service auditor’s report.
  - Determine whether this information has been communicated appropriately to affected user entities. If the information has not been so communicated, and management of the service organization is unwilling to do so, the service auditor should take appropriate action.

Proposed Changes to Service Organization Audits

- Overall Changes to Attestation Standards – Clarification
- Specific Changes Proposed by Task Force
  - Align with Chapters 1-4 of attestation standards
  - Revise definition of *complementary user entity controls* to limit the definition to controls that are necessary to achieve the control objectives stated in management's description of the service organization's system.

Proposed Changes To Service Organization Audits (cont’d)

- Introduce the term *complementary subservice organization controls* - controls that management of the service organization expects, in the design of the services provided by the subservice organization, will be implemented by carved-out subservice organizations, and are necessary to achieve the control objectives stated in management’s description of the service organization’s system.
- Revise material related to using the work of internal auditors and using internal auditors to provide direct assistance to align with final AU-C section 610, *Using the Work of Internal Auditors.*

Questions